ISBN 82-553-0353-7 1978

Mathematics
No 10 - September

# SYMMETRIC SHIFT REGISTERS
## PART 2

by

Jan Søreng
Oslo

PREPRINTS SERIES - Matematisk institutt, Universitetet i Oslo

## Abstract

We study symmetric shift registers defined by

$$(x_1,\ldots,x_n) \to (x_2,\ldots,x_n,x_{n+1})$$

where $x_{n+1} = x_1 + S(x_2,\ldots,x_n)$ and $S$ is a symmetric polynomial over the field $GF(2)$.


## Introduction

In this paper we study symmetric shift registers over the field $GF(2) = \{0,1\}$. In [2] we introduced the block structure of elements in $\{0,1\}^n$ and developed a theory about this block structure. In this paper we will use the results in [2] about the block structure to determine the cycle structure of the symmetric shift registers.

The symmetric shift register $\theta_S$ corresponding to $S(x_2,\ldots,x_n)$ where $S$ is a symmetric polynomial, is defined by

$$\theta_S(x_1,\ldots,x_n) = (x_2,\ldots,x_{n+1}) \quad \text{where} \quad x_{n+1} = x_1 + S(x_2,\ldots,x_n).$$

$q$ is the minimal period of $A \in \{0,1\}^n$ with respect to $\theta_S$ if $q$ is the least integer such that $\theta_S^q(A) = A$. Then $A \to \theta_S(A) \to \ldots \to \theta_S^q(A) = A$ is called the cycle corresponding to $A$. We will for all $S$ solve the following three problems:

1. Determine the minimal period for each $A \in \{0,1\}^n$.
2. Determine the possible minimal periods.
3. Determine the number of cycles corresponding to each minimal period.

Moreover, the problems will be solved in a constructive way, a way which will describe how the minimal periods and the number of cycles can be calculated. In [1] (see also [2]) we reduced all the problems to the case $S = E_k + \ldots + E_{k+p}$ where $E_i$ is defined by

$$E_i(x_2,\ldots,x_n) = 1 \quad \text{if and only if} \quad \sum_{j=2}^{n} x_j = i .$$

In this paper we will only study $S = E_k + \ldots + E_{k+p}$.

I will now roughly describe the structure of the proof. First we need a definition. Suppose $\mathfrak{M} \subset \{0,1\}^n$ is a set such that for all $A \in \mathfrak{M}$ there exists an $i > 0$ such that $\theta_S^i(A) \in \mathfrak{M}$. Then we define $\text{Index} : \mathfrak{M} \to \{1,2,\ldots\}$ and $\psi : \mathfrak{M} \to \mathfrak{M}$ in the following way:

Let $i > 0$ be the least integer such that $\theta_S^i(A) \in \mathfrak{M}$, then we define $\text{Index}(A) = i$ and $\psi(A) = \theta_S^i(A)$.

In the proof we need only consider certain subsets $\mathfrak{M}$ which can be represented in a nice way. We will find for each $A \in \mathfrak{M}$ a minimal $q > 0$ such that $\psi^q(A) = A$. Then

$$\text{Index}(A) + \text{Index}(\psi(A)) + \ldots + \text{Index}(\psi^{q-1}(A))$$

is the minimal period of $A$.

We give now a short outline of the paper. Section 2 contains some definitions and notations. In Section 3 we study a function $\Lambda$ which we need later. In Section 4 we compute $\psi$ for a certain subset $\mathfrak{M}$. In the Sections 5, 6 and 7 we solve the problems 1, 2 and 3 respectively for the set $\mathfrak{M}$. In Section 8 we generalize the results to all $A \in \{0,1\}^n$. This generalization will not be difficult.

[2] is revised. In an appendix we give a summary of the new results in the revised version.

## 2. Preliminaries

We must repeat some of the definitions from [2]. First we define the blocks of $A \in \{0,1\}^n$ ([2],Def.3.1). Intuitively an i-block is i consecutive 1's in A. $0_i$ denotes i consecutive 0's in A and $1_i$ denotes i consecutive 1's in A for $i \geq 0$.

We need some notation. We write $a_1 \ldots a_n = (a_1,\ldots,a_n) \in \{0,1\}^n$. If $A = a_1 \ldots a_n \in \{0,1\}^n$, we define

$$f(a_i \ldots a_j) = (\text{the number of 1's in } a_i \ldots a_j) - (\text{the number of 0's in } a_i \ldots a_j).$$

Moreover, $a \wedge b$ denotes the minimum of a and b.

We divide the definition of blocks into two parts by first defining 1-structures and 0-structures of A. A 1-structure (0-structure) is a generalization of q consecutive 1's (respectively 0's) which is succeeded by q 0's (respectively 1's).

Def. 2.1: With respect to p we define that $D = a_r \ldots a_s$ is a 1-structure of mass q of $A^* = a_1 \ldots a_n a_{n+1} \ldots a_{n+p+1} \in \{0,1\}^{n+p+1}$ if the following 3 conditions are satisfied:

1) $0 < f(a_r \ldots a_i) \leq f(a_r \ldots a_s) = q$ for $i \in \{r,\ldots,s\}$.

2) There exists $t > s$ such that
$0 > f(a_{s+1} \ldots a_i) \geq f(a_{s+1} \ldots a_t) = -q \wedge (p+1)$ for $i \in \{s+1,\ldots,t\}$.

3) If $a_i \ldots a_j < a_r \ldots a_s$, then $f(a_i \ldots a_j) > -q \wedge (p+1)$.

D is a 0-structure of mass q if D satisfies 1), 2) and 3) with f replaced by -f.

3) implies that the 0's in a 1-structure (respectively the 1's in a 0-structure) are not too close to each other. If $q \leq p+1$, then 3) follows from 1) by using $f(a_r \ldots a_i \ldots a_j) = f(a_r \ldots a_i) + f(a_{i+1} \ldots a_j)$.

Def. 2.2: Suppose $A = a_1 \ldots a_n \in \{0,1\}^n$. Let $A^* = a_1 \ldots a_n a_{n+1} \ldots a_{n+p+1} = A0_{p+1}$. We define the blocks in $A^*$ with respect to $p$ by induction with respect to the level of the blocks:

Basisstep: $A^*$ is a block on level 0.

Inductionstep: Suppose $B$ is a block on level $i$. If $i \in \{0,2,4,\ldots\}$, we can decompose $B$ (uniquely) in the following way:

$$B \equiv 0_{i_1} B_1 0_{i_2} B_2 \ldots B_m 0_{i_{m+1}} \quad \text{where } B_i \text{ is a 1-structure.}$$

If $i$ is odd, we can decompose $B$ (uniquely) in the following way:

$$B = 1_{i_1} B_1 1_{i_2} B_2 \ldots B_m 1_{i_{m+1}} \quad \text{where } B_i \text{ is a 0-structure.}$$

By definition $B_i$ is a block on level (i+1). We denote the mass of $B_i$ by $m(B_i)$. We define $\text{type}(B_i) = m(B_i) \wedge (p+1)$.

By definition {the blocks of $A$} are {the blocks of $A^*$}$\setminus${$A^*$}.

We establish the convention that $B$ always denotes a block. Moreover, we suppose $k$ and $p$ are fixed integers such that $0 \leq k \leq k+p \leq n-1$. The block structure is always determined with respect to $p$ and we always work with $S = E_k + \ldots + E_{k+p}$. We write $\theta = \theta_S$. These conventions do not concern Section 8.

If $A = a_1 \ldots a_n$, we write $l_A(a_i \ldots a_j) = i$ and $r_A(a_i \ldots a_j) = j$. Next we define $d(B)$ which measures how far the block $B$ is to the left in $A$. Suppose $A = a_1 \ldots a_n$. We

define

$$d_q(a_1 \dots a_j) = j - \Sigma\{q \wedge \text{type}(B) : l_A(B) \leq j\} - \Sigma\{q \wedge \text{type}(B) : r_A(B) \leq j\}.$$

If $B$ is a block of $A$, then we define $d(B) = 0$ if $l_A(B)=1$. Otherwise,

$$d(B) = d_q(a_1 \dots a_j) \quad \text{where} \quad j = l_A(B) - 1 \quad \text{and} \quad q = \text{type}(B).$$

Moreover, we define $w(\cdot)$ by $w(a_1 \dots a_n) = \sum_{i=1}^{n} a_i$.

## 3. The function $\Lambda$.

In this section we study the functions $\Lambda(\alpha)$ and $\Lambda(\alpha,m)$. We will use these functions to formulate and study how $d(B)$ (the distance of a block $B$) changes by applying the shift register.

Def. 3.1: a) For $(t_1,\dots,t_\gamma) \in \mathfrak{D}(\alpha) = \{(t_1,\dots,t_\gamma) : 1 \leq t_1 \leq \dots \leq t_\gamma \leq \alpha\}$ we define

$$\Lambda(\alpha)(t_1,\dots,t_\gamma) = (t_i-1,\dots,t_\gamma-1,\alpha,\dots,\alpha) \in \{1,2,\dots,\alpha\}^\gamma$$

where $i$ is the least index such that $t_i > 1$. Specially, $\Lambda(\alpha)(1,\dots,1) = (\alpha,\dots,\alpha)$.

b) We define $\mathfrak{D}(\alpha,m)$ by

$$\left[\binom{t_1}{s_1},\dots,\binom{t_\gamma}{s_\gamma}\right] \in \mathfrak{D}(\alpha,m)$$

if and only if

$$0 \leq t_1 \leq t_2 \dots \leq t_\gamma \leq \alpha$$
$$t_i+s_i \leq t_{i+1} \quad \text{for} \quad i = 1,\dots,\gamma-1$$
$$t_\gamma+s_\gamma = \alpha$$
$$s_i \geq 0 \quad \text{and} \quad s_1+\dots+s_\gamma = m.$$

For $\vec{t} = [\binom{t_1}{s_1},\dots,\binom{t_\gamma}{s_\gamma}] \in \mathfrak{D}(\alpha,m)$ we define

$$\Lambda(\alpha,m)(\vec{t}) = \left[\binom{t_2-t_1-s_1}{s_2},\binom{t_3-t_1-s_1}{s_3},\ldots,\binom{t_\gamma-t_1-s_1}{s_\gamma},\binom{\alpha-s_1}{s_1}\right]$$

We observe that $\Lambda(\alpha)\colon \mathcal{D}(\alpha) \to \mathcal{D}(\alpha)$ and $\Lambda(\alpha,m)\colon \mathcal{D}(\alpha,m) \to \mathcal{D}(\alpha,m)$. We will now indicate how to use these functions. First we need a definition.

Def. 3.2: Suppose $B_1,\ldots,B_\gamma$ are the i-blocks of $A \in \{0,1\}^n$ ordered from the left to the right. We define

$$D_i(A) = (d(B_1),\ldots,d(B_\gamma)) \quad \text{if} \quad i \leq p .$$

$$D_{p+1}(A) = \left[\binom{d(B_1)}{m(B_1)-(p+1)},\ldots,\binom{d(B_\gamma)}{m(B_\gamma)-(p+1)}\right] \quad \text{if} \quad i = p+1 .$$

The vectors $D_1(A),\ldots,D_{p+1}(A)$ determine the blockstructure of $A$ completely. In the next sections we will study a subset $\mathfrak{M} \subset \{0,1\}^n$ where it is possible to define $\psi$ as in the introduction. For each $A \in \mathfrak{M}$ and $q > 0$ we will determine integers $\alpha_i$, $m$ and $\beta_i$ such that ($\alpha_i$ and $m$ will be independent of $q$)

$$D_i(\psi^q(A)) = \Lambda(\alpha_i)^{\beta_i}(D_i(A)) \quad \text{for} \quad i = 1,\ldots,p \quad \text{and}$$

$$D_{p+1}(\psi^q(A)) = \Lambda(\alpha_{p+1},m)^{\beta_{p+1}}(D_{p+1}(A)) .$$

We will now prove two lemmas which determine when $\vec{t} = \Lambda(\alpha)^\beta(\vec{t})$ and $\vec{t} = \Lambda(\alpha,m)^\beta(\vec{t})$.

Def. 3.3: a) The difference vector of $\vec{t} = (t_1,\ldots,t_\gamma)$ with respect to $\alpha$ is

$$(\alpha+t_1-t_\gamma,\ t_2-t_1,\ t_3-t_2,\ldots,t_\gamma-t_{\gamma-1}) .$$

b) The difference vector of $t = [\binom{t_1}{s_1},\ldots,\binom{t_\gamma}{s_\gamma}]$ with respect to $\alpha$ is

$$\left[\binom{\alpha+t_1-t_\gamma}{s_1},\binom{t_2-t_1}{s_2},\binom{t_3-t_2}{s_3},\ldots,\binom{t_\gamma-t_{\gamma-1}}{s_\gamma}\right].$$

Def. 3.4: The trivial period of $(r_1,\ldots,r_\gamma)$ is the least integer $\gamma^* > 0$ such that $(r_1,\ldots,r_\gamma) = (r_{\gamma^*+1},\ldots,r_\gamma,r_1,\ldots,r_{\gamma^*})$.

Lemma 3.5: Suppose $\gamma^*$ is the trivial period of the difference vector of $\vec{t} = (t_1,\ldots,t_\gamma) \in \mathfrak{D}(\alpha)$ with respect to $\alpha$.

Then $\gamma/\gamma^*$ and $\alpha^* = \alpha\cdot\gamma^*/\gamma$ are integers. Moreover,

$$\Lambda(\alpha)^\beta(\vec{t}) = \vec{t} \iff \beta = 0 \text{ modulo } \alpha^*.$$

We write $\gamma^* = \gamma^*(\alpha,\vec{t})$ and $\alpha^* = \alpha^*(\alpha,\vec{t})$.

Proof: We denote the difference vector of $\vec{t}$ with respect to $\alpha$ by

$$(r_1,\ldots,r_\gamma) = (\alpha+t_1-t_\gamma,t_2-t_1,\ldots,t_\gamma-t_{\gamma-1}).$$

We get

$$\sum_{j=1}^{\gamma} r_j = (\alpha+t_1-t_\gamma) + (t_2-t_1) + \ldots +(t_\gamma-t_{\gamma-1}) = \alpha.$$

By the hypothesis $\gamma = s\gamma^*$ for an integer $s$ and

$$r_1+\ldots r_{\gamma^*} = r_{\gamma^*+1}+\ldots+r_{2\gamma^*} = \ldots = r_{(s-1)\gamma^*+1}+\ldots+r_{s\gamma^*}.$$

Hence, $r_1+\ldots+r_{\gamma^*} = \alpha/s = \alpha\cdot\gamma^*/\gamma = \alpha^*$ is an integer.

We will now prove

$$(3.1)\quad \begin{cases} t_j-t_{j-\gamma^*} = \alpha^* & \text{for } \gamma^* < j \le \gamma. \\ t_j-t_{j-\gamma^*+\gamma} = \alpha^*-\alpha & \text{for } 1 \le j \le \gamma^*. \end{cases}$$

If $\gamma^* < j \leq \gamma$, then

$$t_j - t_{j-\gamma^*} = \sum_{i=1}^{\gamma^*} (t_{j-\gamma^*+i} - t_{j-\gamma^*+i-1}) = \sum_{i=1}^{\gamma^*} r_{j-\gamma^*+i} = \alpha^* .$$

If $1 \leq j \leq \gamma^*$, then

$$t_j - t_{j-\gamma^*+\gamma} + \alpha = \sum_{i=1}^{\gamma^*-j} (t_{j-\gamma^*+\gamma+i} - t_{j-\gamma^*+\gamma+i-1}) + (t_1 - t_\gamma + \alpha)$$

$$+ \sum_{i=2}^{j} (t_i - t_{i-1}) = r_{\gamma-\gamma^*+j+1} + \ldots + r_\gamma + r_1 + \ldots + r_j = \alpha^*,$$

and the proof of (3.1) is complete.

Next, we compute $\Lambda(\alpha)^{\alpha^*}(\vec{t})$. Since $t_1 > 0$ and by using (3.1) we get

(3.2) $\quad t_{\gamma^*} = t_\gamma + \alpha^* - \alpha \leq \alpha^*$ and $t_{\gamma^*+1} = t_1 + \alpha^* > \alpha^*$.

Hence, by definition

$$\Lambda(\alpha)^{\alpha^*}(\vec{t}) = (t_{\gamma^*+1} - \alpha^*, \ldots, t_\gamma - \alpha^*, t_1 + \alpha - \alpha^*, \ldots, t_{\gamma^*} + \alpha - \alpha^*) .$$

By using (3.1) we get $\Lambda(\alpha)^{\alpha^*}(\vec{t}) = \vec{t}$.

Finally, we will prove that $\Lambda(\alpha)^{\beta}(\vec{t}) = \vec{t}$ implies $\beta = 0$ modulo $\alpha^*$. It is sufficient to prove that $0 \leq \beta \leq \alpha^*$ implies $\beta = 0$ or $\beta = \alpha^*$. Let $i$ be the maximal $i$ such that $t_i \leq \beta$. By definition

$$\Lambda(\alpha)^{\beta}(\vec{t}) = (t_{i+1} - \beta, \ldots, t_\gamma - \beta, t_1 + \alpha - \beta, \ldots, t_i + \alpha - \beta) .$$

Hence,

(3.3) $\quad$ the difference vector of $\Lambda(\alpha)^{\beta}(\vec{t})$ with respect to $\alpha$ is $(r_{i+1}, \ldots, r_\gamma, r_1, \ldots, r_i)$.

Hence, $(r_1, \ldots, r_\gamma) = (r_{i+1}, \ldots, r_\gamma, r_1, \ldots, r_i)$. By the hypothesis $i = 0$ or $i = \gamma^*$. If $i = \gamma^*$, we get by (3.1) that $t_{\gamma^*+1} - \beta = t_1 = t_{\gamma^*+1} - \alpha^*$. If $i = 0$, then $t_1 - \beta = t_1$. Hence, $\beta = \alpha^*$ or $\beta = 0$.

Q.E.D.

Lemma 3.6: Suppose $\gamma^*$ is the trivial period of the difference vector of $\vec{t} = [\binom{t_1}{s_1},\ldots,\binom{t_\gamma}{s_\gamma}] \in \mathcal{D}(\alpha,m)$ with respect to $\alpha$.

Then $\gamma/\gamma^*$, $\alpha^* = \alpha\cdot(\gamma^*/\gamma)$ and $m\cdot(\gamma^*/\gamma)$ are integers, Moreover,

$$\Lambda(\alpha,m)^\beta(\vec{t}) = \vec{t} \iff \beta = 0 \text{ modulo } \gamma^*.$$

We write $\gamma^* = \gamma^*(\alpha,\vec{t})$ and $\alpha^* = \alpha^*(\alpha,\vec{t})$.

Proof: As in the proof of Lemma 3.5 we prove that $\gamma/\gamma^*$, $\alpha^* = (\gamma^*/\gamma)\cdot\alpha$ and $(\gamma^*/\gamma)\cdot m$ are integers. Moreover, (3.1) is true and $s_j = s_i$ when $j = i$ modulo $\gamma^*$.

By induction

$$(3.4)\qquad \Lambda(\alpha,m)^i(\vec{t}) = \left[\binom{t_{i+1}-(s_i+t_i)}{s_{i+1}},\binom{t_{i+2}-(s_i+t_i)}{s_{i+2}},\cdots\right] \text{ for } i=1,\ldots,\gamma^*.$$

By (3.1) and since $\gamma^* = \gamma$ modulo $\gamma^*$, we get $s_{\gamma^*}+t_{\gamma^*} = s_\gamma+(t_\gamma+\alpha^*-\alpha)$. By the definition of $\mathcal{D}(\alpha,m)$ we have $s_\gamma+t_\gamma = \alpha$. Hence, $s_{\gamma^*}+t_{\gamma^*} = \alpha^*$. Therefore,

$$\Lambda(\alpha,m)^{\gamma^*}(\vec{t}) = \left[\binom{t_{\gamma^*+1}-\alpha^*}{s_{\gamma^*+1}},\ldots,\binom{t_\gamma-\alpha^*}{s_\gamma},\binom{t_1+\alpha-\alpha^*}{s_1},\ldots,\binom{t_{\gamma^*}+\alpha-\alpha^*}{s_{\gamma^*}}\right].$$

By (3.1) we get $\Lambda(\alpha,m)^{\gamma^*}(\vec{t}) = \vec{t}$.

Suppose $\Lambda(\alpha,m)^j(\vec{t}) = \vec{t}$. It is sufficient to prove that $0 \le j \le \gamma^*$ implies $j = 0$ or $j = \gamma^*$. By definition there exists an integer $a \ge 0$ such that

$$\Lambda(\alpha,m)^j(\vec{t}) = \left[\binom{t_{j+1}-a}{s_{j+1}},\ldots,\binom{t_\gamma-a}{s_\gamma},\binom{t_1+\alpha-a}{s_1},\ldots,\binom{t_j+\alpha-a}{s_j}\right]$$

If $[\binom{r_1}{s_1},\ldots,\binom{r_\gamma}{s_\gamma}]$ is the difference vector of $\vec{t}$, then

$\left[\binom{r_{j+1}}{s_{j+1}},\ldots,\binom{r_\gamma}{s_\gamma},\binom{r_1}{s_1},\ldots,\binom{r_j}{s_j}\right]$ is the difference vector of $\Lambda(\alpha,m)^j(\vec{t})$. By the hypothesis, $j = 0$ or $j = \gamma^*$.

Q.E.D.

Later we will also need the following definition and lemmas.

Def. 3.7: Suppose $\vec{t} = (t_1,\ldots,t_\gamma) \in \mathfrak{D}(\alpha)$ and $0 \leq \beta \leq \alpha$. If $t_1 > \beta$, we define $r(\beta,\vec{t}) = 0$. Otherwise $r(\beta,\vec{t})$ is the maximal integer $r$ such that $t_r \leq \beta$.

Lemma 3.8: Suppose $\vec{t} \in \mathfrak{D}(\alpha)$ and $\alpha^* = \alpha^*(\alpha,\vec{t})$ and $\gamma^* = \gamma^*(\alpha,\vec{t})$. Suppose $0 \leq \beta_i \leq \alpha$ and $\beta_0+\ldots+\beta_{s-1} = X\cdot\alpha^*$.
Then

$$r(\beta_0,\vec{t}) + \sum_{i=1}^{s-1} r(\beta_i,\Lambda(\alpha)^{\beta_0+\ldots+\beta_{i-1}}(\vec{t})) = X\cdot\gamma^*.$$

Proof: Suppose $0 \leq \beta_0 + \beta_1 \leq \alpha$. We observe that

$$(3.5)\quad r(\beta_0+\beta_1,\vec{t}) = r(\beta_0,\vec{t}) + r(\beta_1,\Lambda(\alpha)^{\beta_0}(\vec{t})).$$

(3.2) in the proof of Lemma 3.5 implies $r(\alpha^*,\vec{t}) = \gamma^*$. Hence, the case $X = 1$ follows from (3.5).

If $X > 1$, we choose $q$ such that $\beta_0+\ldots+\beta_{q-1} < \alpha^*$ and $\beta_0+\ldots+\beta_q > \alpha^*$. We choose $\beta'$ and $\beta''$ such that $\beta'+\beta'' = \beta_q$ and $\beta_0+\ldots+\beta_{q-1}+\beta' = \alpha^*$. The claim follows by induction with respect to $X$ by studying $\beta_0+\ldots+\beta_{q-1}+\beta'+\beta''+\beta_{q+1}+\ldots+\beta_{s-1}$.

Q.E.D.

Lemma 3.9: Suppose $\vec{t} \in \mathfrak{D}(\alpha,m)$ and $\alpha^* = \alpha^*(\alpha,\vec{t})$ and $\gamma^* = \gamma^*(\alpha,\vec{t})$. We denote

$$\Lambda(\alpha,m)^i(t) = \left[\binom{t_1^i}{s_1^i},\ldots,\binom{t_\gamma^i}{s_\gamma^i}\right]. \text{ Then } \sum_{i=0}^{X\cdot\gamma^*-1}(t_1^i+s_1^i) = X\cdot\alpha^*.$$

Proof: By (3.4) and $t_1^0+s_1^0 = t_1+s_1$ we get

$$\sum_{i=0}^{\gamma^*-1}(t_1^i+s_1^i) = (t_1+s_1)+\sum_{i=1}^{\gamma^*-1}[(t_{i+1}-(t_i+s_i))+s_{i+1}] = t_{\gamma^*}+s_{\gamma^*} = \alpha$$

The last equality is proved in the proof of Lemma 3.6.

Q.E.D.

Finally, we do the following observation.

Observation 3.10: If $\vec{t} \in \mathcal{D}(\alpha)$, then the trivial periods of the difference vectors of $\vec{t}$ and $\Lambda(\alpha)^i(\vec{t})$ are equal.

If $\vec{t} \in \mathcal{D}(\alpha,m)$, then the trivial periods of the difference vectors of $\vec{t}$ and $\Lambda(\alpha,m)^i(\vec{t})$ are equal.

This observation follows from (3.4) and the proof of Lemma 3.6.

## 4. Computation of $\psi$.

We will in Section 4 - 7 study the set $\mathfrak{M} \subset \{0,1\}^n$ defined by

$$A \in \mathfrak{M} \iff \begin{cases} A \text{ ends with a } (p+1)\text{-block.} \\ A \text{ starts with } 0 \text{ or a } (p+1)\text{-block.} \\ w(A) = k+p+1 \ . \end{cases}$$

By lemma 4.11 and 4.13 in [2] there exists an $i > 0$ such that $\theta^i(A) \in \mathfrak{M}$ for all $A \in \mathfrak{M}$. We define $\text{Index} : \mathfrak{M} \to \{1,2,\ldots\}$ and $\psi : \mathfrak{M} \to \mathfrak{M}$ in the following way:

Let $i > 0$ be the least integer such that $\theta^i(A) \in \mathfrak{M}$, then we define $\text{Index}(A) = i$ and $\psi(A) = \theta^i(A)$.

In [2] we denoted $\psi$ by $\varphi_{min}$. If $A \in \mathfrak{M}$ contains 1 (p+1)-block, we also denoted $\psi$ by $\varphi$ in [2]. We get the following lemma:

Lemma 4.1: If $A \in \mathfrak{M}$ and $q$ is the least integer $q > 0$ such that $\psi^q(A) = A$, then $\mathrm{Index}(A) + \ldots + \mathrm{Index}(\psi^{q-1}(A))$ is the minimal period of $A$ with respect to $\theta$.

First we will reformulate how $\psi$ works. Lemma 4.2 and 4.3 are reformulations of Lemma 4.11 and 4.13 in [2] respectively.
We define

$$(4.1)\quad \begin{cases} \gamma_i(A) = \text{the number of } i\text{-blocks in } A. \\ \alpha_i(A) = n+i - \sum_{j=1}^{i} 2j \cdot \gamma_j(A) - 2i \cdot \sum_{j=i+1}^{p+1} \gamma_j(A) . \end{cases}$$

Moreover, $D_i(A)$ is defined in Def. 3.2.

Lemma 4.2: Suppose $A \in \mathfrak{M}$ contains 1 $(p+1)$-block. We let $\alpha_i = \alpha_i(A)$ for $i = 1, \ldots, p+1$. We define $r_q = r_q(A)$ and $\beta_q = \beta_q(A)$ inductively for $q = 1, \ldots, p$ by the formulaes:

$\beta_p = 1$, $\beta_q = (p+1-q) + \sum_{i=q+1}^{p} 2 \cdot (i-q) \cdot r_i$ and

$r_q$ = the number of $q$-blocks $B$ in $A$ such that

$$d(B) \leqq \beta_q \quad (r_q = r(\beta_q, D_q(A))) .$$

Then $D_{p+1}(\psi(A)) = D_{p+1}(A)$. If $\gamma_i(A) \neq 0$ and $1 \leqq i \leqq p$, then $D_i(A) \in \mathfrak{D}(\alpha_i)$ and $D_i(\psi(A)) = \Lambda(\alpha_i)^{\beta_i}(D_i(A))$.

Moreover,

$$\mathrm{Index}(A) = n+p+1 + \sum_{i=1}^{p} 2 \cdot i \cdot r_i \leqq 2n .$$

Proof: By Lemma 4.1 c) in [2] we have $D_i(A) \in \mathfrak{D}(\alpha_i)$ for $i = 1, \ldots, p$. $\varphi(A)$ in Lemma 4.11 in [2] is equal to $\psi(A)$. By Lemma 4.11 b) and d)

in [2] $\beta_q = \chi_q(A)$ and $r_q$ is identical with the $r_q$ in Lemma 4.11 in [2]. Then it is not difficult to see that this lemma is a reformulation of Lemma 4.11 in [2].

Q.E.D.

Lemma 4.3: Suppose $A \in \mathfrak{M}$ contains more than 1 (p+1)-block. Let

$m = m_A = \Sigma\{m(B) - (p+1): B \text{ is a } (p+1) - \text{block in } A\}$ .

Suppose $B_F$ is the first (p+1)-block in A .

Moreover, $\alpha_i = \alpha_i(A)$ for $i = 1,\cdots,p+1$ .

We define $r_q = r_q(A)$ $(q=1,\cdots,p+1)$ and $\beta_q = \beta_q(A)$ $(q=1,\cdots,p)$ inductively by the formulaes

$$r_{p+1} = 1 ,$$

$$\beta_q = [d(B_F) + m(B_F) - (p+1)] + \sum_{i=q+1}^{p+1} 2\cdot(i-q)\cdot r_i ,$$

and for $q = 1,\cdots,p$ :

$r_q$ = the number of q-blocks B in A such that $d(B) \leqq \beta_q$ $(r_q = r(\beta_q, D_q(A)))$ .

Then we have

$D_{p+1}(A) \in \mathfrak{D}(\alpha_{p+1}, m)$ and $D_{p+1}(\psi(A)) = \Lambda(\alpha_{p+1}, m)(D_{p+1}(A))$ .

If $\gamma_i(A) \neq 0$ and $1 \leqq i \leqq p$ , then we have $D_i(A) \in \mathfrak{D}(\alpha_i)$ and

$D_i(\psi(A)) = \Lambda(\alpha_i)^{\beta_i}(D_i(A))$ .

Moreover,

$$\text{Index } (A) = [d(B_F) + m(B_F) - (p+1)] + \sum_{i=1}^{p+1} 2i\cdot r_i \leqq n .$$

Proof: By Lemma 4.1 c) in [2] we have $D_i(A) \in \mathfrak{D}(\alpha_i)$ for $i = 1,\ldots,p$ and $D_{p+1}(A) \in \mathfrak{D}(\alpha_{p+1}, m)$ .

$\varphi_{min}(A)$ in Lemma 4.13 in [2] is equal to $\psi(A)$ . It is easy to see that this Lemma follows from Lemma 4.13 in [2] .

Q.E.D.

In the forthcoming proof we represent the elements of $\mathfrak{M}$ by

$$\pi(A) = D_1(A) \times \cdots \times D_{p+1}(A) .$$

It is easy to define $\psi_\pi$ and $\mathrm{Index}_\pi$ on $\pi(\mathfrak{M})$ such that $\psi_\pi \circ \pi = \pi \circ \psi$ and $\mathrm{Index}_\pi \circ \pi = \pi \circ \mathrm{Index}$ , and study $\psi_\pi$ and $\mathrm{Index}_\pi$ instead of $\psi$ and Index . By using $\mathrm{Index}_\pi$ and $\psi_\pi$ the structure of the proof would be somewhat clearer. But to avcid complicated notation we do not do so.

In the next section we will calculate $\psi^i(A)$ for certain $i$ . In these calculations we need the following lemma.
First we need a definition

$$(4.2) \quad \beta_q^s(A) = \beta_q(A) + \beta_q(\psi(A)) + \cdots + \beta_q(\psi^{s-1}(A)) .$$

Def. 4.4: For each $A \in \mathfrak{M}$ we define $\gamma_i^*(A) = \gamma^*(\alpha_i(A), D_i(A))$ and $\alpha_i^*(A) = \alpha^*(\alpha_i(A), D_i A))$ .

Lemma 4.5: We suppose $A \in \mathfrak{M}$. Let $\gamma_i = \gamma_i(A)$ , $\gamma_i^* = \gamma^*(A)$ and $\alpha_i^* = \alpha_i^* = \alpha_i^*(A)$ . Moreover, we suppose
for $t \in \{q+1, \cdots, p\}$ :

$$\beta_t^Y(A) = X_t \cdot \alpha_t^* \quad \text{if} \quad \gamma_t \neq 0 .$$

$$X_t = 0 \quad \text{if} \quad \gamma_t = 0 .$$

a) If $\gamma_{p+1} = 1$ , then

$$\beta_q^Y(A) = Y(p+1-q) + \sum_{t=q+1}^{P} 2 \cdot (t-q) \cdot X_t \cdot \gamma_t^* .$$

b) If $\gamma_{p+1} > 1$ and $Y = X_{p+1} \cdot \gamma_{p+1}^*$ , then

$$\beta_q^Y(A) = X_{p+1}\ \alpha_{p+1}^* + \sum_{t=q+1}^{p+1} 2 \cdot (t-q) \cdot X_t \cdot \gamma_t^* .$$

Proof: Suppose $\gamma_t \neq 0$ . We write $\beta_{t,s} = \beta_t(\psi^s(A))$ . By

Lemma 4.2 and 4.3 we get

$$(4.3)\quad D_t(\psi^s(A)) = \Lambda(\alpha_t)^{\beta_{t,0}+\cdots+\beta_{t,s-1}}(D_t(A)) .$$

By the hypothesis

$$(4.4)\quad \beta_{t,0}+\cdots+\beta_{t,Y-1} = X_t\cdot\alpha_t^* .$$

We have $D_t(A) \in \mathfrak{D}(\alpha_t)$, $\alpha_t^* = \alpha^*(\alpha_t, D_t(A))$ and $\gamma_t^* = \gamma^*(\alpha_t, D_t(A))$ . Hence, by (4.3), (4.4) and Lemma 3.8 we get

$$(4.5)\quad \sum_{s=0}^{Y-1} r_t(\psi^s(A)) = \sum_{s=0}^{Y-1} r(\beta_{t,s}, D_t(\psi^s(A)) = X_t\cdot\gamma_t^* .$$

<u>The proof of a)</u>: By Lemma 4.2 and (4.5) we get

$$\beta_q^Y(A) = \sum_{s=0}^{Y-1}\beta_q(\psi^s(A)) = \sum_{s=0}^{Y-1}\Big[p+1-q+\sum_{t=q+1}^{P}2(t-q)\cdot r_t(\psi^s(A))\Big]$$

$$= Y(p+1-q) + \sum_{t=q+1}^{P}2(t-q)\cdot X_t\cdot\gamma_t^* .$$

<u>The proof of b)</u>: By Lemma 4.3 we get

$$(4.6)\quad r_{p+1}(\psi^j(A)) = 1 \quad \text{for all } j .$$

We write

$$D_{p+1}(\psi^j(A)) = [\binom{t_1^j}{s_1^j},\cdots] .$$

(If $B_F^j$ is the first (p+1)-block in $\psi^j(A)$ , then $t_1^j = d(B_F^j)$ and $s_1^j = m(B_F^j) - (p+1)$ .)

Since $Y = X_{p+1}\gamma_{p+1}^*$ we have by Lemma 3.9

$$(4.7)\quad \sum_{j=0}^{Y-1}(t_1^j+s_1^j) = X_{p+1}\cdot\alpha_{p+1}^* .$$

By (4.5), (4.6), (4.7) and Lemma 4.3 we get

$$\beta_q^Y(A) = \sum_{j=0}^{Y-1} \beta_q(\psi^j(A))$$

$$= \sum_{j=0}^{Y-1} [t_1^j + s_1^j + \sum_{t=q+1}^{p+1} 2(t-q) \cdot r_t(\psi^j(A))]$$

$$= \alpha_{p+1}^* \cdot X_{p+1} + \sum_{t=q+1}^{p+1} 2(t-q) \cdot X_t \gamma_t^* + 2(p+1-q) \cdot Y .$$

Since $Y = X_{p+1}\gamma_{p+1}^*$ the proof is complete.

Q.E.D.

## 5. How to determine the minimal period.

We will now determine the minimal periods of $A \in \mathcal{M}$. $\gamma_i(A)$ and $\alpha_i(A)$ are defined in (4.1). $D_i(A)$ is defined in Def. 3.2. Moreover, $\gamma_i^*(A)$ and $\alpha_i^*(A)$ are defined in Def. 4.4 and $\mathcal{M}$ is defined in Section 4. We repeat the definitions of $\gamma_i^*(A)$ and $\alpha_i^*(A)$ : Suppose first $1 \leqq i \leqq p$ and $D_i(A) = (t_1, \cdots, t_{\gamma_i})$. Then $\gamma_i^*(A)$ is the trivial period of

$$(t_1 - t_{\gamma_i} + \alpha_i(A),\ t_2 - t_1,\ t_3 - t_2,\ \cdots,\ t_{\gamma_i} - t_{\gamma_i - 1}) .$$

Next we suppose $D_{p+1}(A) = \left[\binom{t_1}{s_1}, \ldots, \binom{t_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\right]$. Let $t' = t_1 - t_{\gamma_{p+1}} + \alpha_{p+1}(A)$ and $t'' = t_{\gamma_{p+1}} - t_{\gamma_{p+1}-1}$. Then $\gamma_{p+1}^*(A)$ is the trivial period of

$$\left[\binom{t'}{s_1}, \binom{t_2 - t_1}{s_2}, \binom{t_3 - t_1}{s_3}, \ldots, \binom{t''}{s_{\gamma_{p+1}}}\right].$$

Moreover, $\alpha_i^*(A) = \alpha_i(A) \cdot (\gamma_i^*(A) / \gamma_i(A))$ for $i = 1, \ldots, p+1$ .

Theorem 5.1: Suppose $A \in \mathfrak{M}$. We let $\gamma_i = \gamma_i(A)$, $\alpha_i = \alpha_i(A)$, $\gamma_i^* = \gamma_i^*(A)$ and $\alpha_i^* = \alpha_i^*(A)$.

If $\gamma_i = 0$ for $i = 1,\cdots,p$ we let $X_{p+1} = 1$ and $X_1 = \cdots = X_p = 0$. Otherwise, we define equation (q) by

$$(q)\quad \begin{cases} \alpha_q^* \cdot X_q = \alpha_{p+1}^* \cdot X_{p+1} + \sum_{i=q+1}^{p+1} 2(i-q)\cdot X_i \cdot \gamma_i^* & \text{if } \gamma_q \neq 0 \\ X_q = 0 & \text{if } \gamma_q = 0, \end{cases}$$

for $q = 1,\ldots,p$. Moreover, we let $X_1,\ldots,X_{p+1}$ be the least positive integral solution of the equations $(1),\ldots,(p)$.

Then $X_{p+1}\alpha_{p+1}^* + \sum_{i=1}^{p+1} 2i\cdot\gamma_i^*\cdot X_i$ is the minimal period of $A$ with respect to the shift register $(x_1,\ldots,x_n) \to (x_2,\ldots,x_{n+1})$ where

$$x_{n+1} = x_1 + (E_k+\ldots+E_{k+p})(x_2,\ldots,x_n).$$

If $\gamma_i = 0$ for $i = 1,\ldots,p$, we observe that the minimal period $= X_{p+1}\alpha_{p+1}^* + 2(p+1)\gamma_{p+1}^* X_{p+1} = \alpha_{p+1}^* + 2(p+1)\gamma_{p+1}^*$

$$= \frac{\gamma_{p+1}^*}{\gamma_{p+1}}(\alpha_{p+1} - 2(p+1)\gamma_{p+1}) = \frac{\gamma_{p+1}^*}{\gamma_{p+1}}(n+p+1).$$

The existence of the minimal solution $X_1,\ldots,X_{p+1}$ is proved as indicated in Section 3 in [2].

Proof: $\beta_q^Y(A)$ is defined in (4.2). We suppose first that $\gamma_{p+1} > 1$. If $\gamma_i \neq 0$ and $i \leq p$, then Lemma 4.3 and 3.5 imply

$$(5.1)\quad \begin{cases} D_i(\psi^Y(A)) = D_i(A) \Leftrightarrow \Lambda(\alpha_i)^{\beta_i^Y(A)}(D_i(A)) = D_i(A) \\ \Leftrightarrow \beta_i^Y(A) = X_i\cdot\alpha_i^* \quad \text{for some } X_i. \end{cases}$$

Moreover, Lemma 4.3 and 3.6 imply ($m = m_A$ is defined in Lemma 4.3)

$$(5.2)\quad \begin{cases} D_{p+1}(\psi^Y(A)) = D_{p+1}(A) \Leftrightarrow \Lambda(\alpha_{p+1},m)^Y(D_{p+1}(A)) = D_{p+1}(A) \\ \Leftrightarrow Y = X_{p+1}\cdot\gamma^*_{p+1} \quad \text{for some} \quad X_{p+1}\ . \end{cases}$$

By Lemma 4.1 in [2] $A$ is uniquely determined by $D_i(A)$ $(i = 1,\ldots,p+1)$. Hence, by (5.1) and (5.2) we get

$$(5.3)\quad \psi^Y(A) = A \Leftrightarrow \begin{cases} \beta_i^Y(A) = X_i\alpha_i^* & \text{when} \quad \gamma_i \neq 0 \quad (i=1,\ldots,p) \text{ and} \\ Y = X_{p+1}\cdot\gamma^*_{p+1}\ . \end{cases}$$

We suppose $\gamma_i \neq 0$ for at least one $i < p+1$. First we will prove

$$(5.4)\quad \{Y:\ \psi^Y(A) = A\} = \{X_{p+1}\gamma^*_{p+1} : X_1,\ldots,X_{p+1} \text{ is a solution of the equations } (1),\ldots,(p)\}\ .$$

Suppose $\psi^Y(A) = A$. By (5.3) there exist $X_1,\ldots,X_{p+1}$ such that

$$Y = X_{p+1}\gamma^*_{p+1} \quad \text{and} \quad \beta_i^Y(A) = X_i\alpha_i^* \quad \text{when} \quad \gamma_i \neq 0 \quad \text{and} \quad i \leqq p\ .$$

If $\gamma_i = 0$, we put $X_i = 0$. We suppose the equations $(q+1),\ldots,(p)$ are satisfied. We suppose $\gamma_q \neq 0$. By Lemma 4.5 b)

$$\beta_q^Y(A) = X_{p+1}\alpha^*_{p+1} + \sum_{t=q+1}^{p+1} 2\cdot(t-q)\cdot X_t\cdot\gamma_t^*\ .$$

Since $\beta_q^Y(A) = X_q\cdot\alpha_q^*$, the equation $(q)$ is satisfied. Hence, $Y = X_{p+1}\gamma^*_{p+1}$ and $X_1,\ldots,X_{p+1}$ satisfy the equations.

Next we suppose $Y = X_{p+1}\gamma^*_{p+1}$ and that $X_1,\ldots,X_{p+1}$ satisfy the equations. We prove by induction

$$(5.5)\quad \beta_i^Y(A) = X_i\cdot\alpha_i^* \quad \text{for} \quad 1 \leqq i \leqq p \quad \text{and} \quad \gamma_i \neq 0\ .$$

We suppose (5.5) is true for $i = q+1,\ldots,p$ and $\gamma_q \neq 0$.

By Lemma 4.5 b) and the equation (q)

$$\beta_q^Y(A) = X_{p+1}\alpha^*_{p+1} + \sum_{t=q+1}^{p+1} 2\cdot(t-q)\cdot\gamma_t^*\cdot X_t = X_q\cdot\alpha_q^* .$$

Hence, the proof of (5.5) is complete. By (5.3) we get $\psi^Y(A) = A$.

Suppose $X_1,\ldots,X_{p+1}$ is the least solution of the equations (1),...,(p). By (5.4)

$Y = X_{p+1}\gamma^*_{p+1}$ is the least $Y$ such that $\psi^Y(A) = A$. By Lemma 4.1 the following sum is the least period of $A$:

$$J(Y) = \sum_{j=o}^{Y-1} \mathrm{Index}(\psi^j(A)) . \tag{5.6}$$

We will now calculate this sum. We suppose $B_F^j$ is the first (p+1)-block in $\psi^j(A)$.

By (4.7) in the proof of Lemma 4.5 we get

$$\sum_{j=o}^{Y-1} (d(B_F^j) + m(B_F^j) - (p+1)) = X_{p+1}\cdot\alpha^*_{p+1} . \tag{5.7}$$

By Lemma 4.3, (5.7) and (4.5) (in the proof of Lemma 4.5) we get

$$\begin{aligned} J(Y) &= \sum_{j=o}^{Y=1} (d(B_F^j) + m(B_F^j) - (p+1) + \sum_{i=1}^{p+1} 2\,i\,r_i(\psi^j(A))) \\ &= X_{p+1}\alpha^*_{p+1} + 2\sum_{i=1}^{p+1} i\cdot\gamma_i^*\cdot X_i . \end{aligned}$$

Next we suppose $\gamma_{p+1} > 1$ and $\gamma_i = 0$ for $i = 1,\ldots,p$. Let $X_{p+1} = 1$ and $X_1 = \ldots = X_p = 0$.

By (5.3) we get

$$Y = X_{p+1}\gamma^*_{p+1} = \gamma^*_{p+1} \text{ is the least } Y \text{ such that } \psi^Y(A) = A . \tag{5.8}$$

We calculate $J(Y)$ in (5.6) as before.

Now we suppose $\gamma_{p+1} = 1$ and $\gamma_i = 0$ for $i = 1,\ldots,p$. It is very easy to see that the least period of $A$ is $n+p+1$. By computation we get $\alpha^*_{p+1}X_{p+1} + \sum_{i=1}^{p+1} 2\cdot i\cdot\gamma_i^*\cdot X_i = n+p+1$, where

$X_{p+1} = 1$ and $X_1 = \ldots = X_p = 0$ .

Finally, we suppose $\gamma_{p+1} = 1$ and $\gamma_i \neq 0$ for at least one $i < p+1$ . We only sketch the proof since the proof is analogous with the case $\gamma_{p+1} > 1$ .

Lemma 4.2 and 3.5 imply that (5.1) is true. By Lemma 4.2 $D_{p+1}(\psi^Y(A)) = D_{p+1}(A)$ . Hence,

$$\psi^Y(A) = A \iff \beta_i^Y(A) = X_i \cdot \alpha_i^* \quad \text{when} \quad \gamma_i \neq 0 \quad \text{and} \quad 1 \leqq i \leqq p .$$

By using Lemma 4.5 a) this is equivalent to: $X_1, \ldots, X_p, Y$ satisfy the equations $(1)', \ldots, (p)'$ given by

$$(q)' \quad \begin{cases} X_q \cdot \alpha_q^* = Y(p+1-q) + \sum_{t=q+1}^{P} 2(t-q) X_t \gamma_t^* & \text{if } \gamma_q \neq 0 \\ X_q = 0 \quad \text{if } \gamma_q = 0 . \end{cases}$$

Let $X_1, \ldots, X_p, Y$ be the least solution of the equations $(1)', \ldots, (p)'$. Then $Y$ is the least $Y$ such that $\psi^Y(A) = A$ . By Lemma 4.2 and (4.5) we calculate the minimal period of $A$ in the following way

$$\sum_{j=0}^{Y-1} \mathrm{Index}(\psi^j(A)) = \sum_{j=0}^{Y-1} [(n+p+1) + 2 \sum_{i=1}^{P} i \cdot r_i(\psi^j(A))]$$

$$= Y(n+p+1) + 2 \sum_{i=1}^{P} i \cdot \gamma_i^* \cdot X_i .$$

The proof will be complete if we can prove the following claim:

Suppose $X_1, \ldots, X_{p+1}$ is the least solution of the equations $(1), \ldots, (p)$ .

Let $Y = X_{p+1}$ and $\hat{X}_t = \begin{cases} 0 & \text{if } \gamma_t = 0 \\ X_t - Y \cdot \frac{\gamma_t}{\gamma_t^*} & \text{if } \gamma_t \neq 0 . \end{cases}$

Then $\hat{X}_1, \ldots, \hat{X}_p, Y$ is the least solution of the equations $(1)', \ldots, (p)'$ , and

$$Y(n+p+1) + \sum_{i=1}^{P} 2i\cdot\hat{X}_i\cdot\gamma_i^* = X_{p+1}\alpha_{p+1}^* + \sum_{i=1}^{p+1} 2i\cdot X_i\cdot\gamma_i^* .$$

Now we will prove this claim. Since $\gamma_{p+1} = \gamma_{p+1}^* = 1$, then $\alpha_{p+1} = \alpha_{p+1}^*$. We use the definition of $\alpha_{p+1}$ and get

$$X_{p+1}\alpha_{p+1}^* + \sum_{i=1}^{p+1} 2i\cdot X_i\cdot\gamma_i^* = Y(n+p+1 - \sum_{i=1}^{p+1} 2i\,\gamma_i)$$

$$+ \sum_{i=1}^{P} 2i\,\gamma_i^*(\hat{X}_i + Y\frac{\gamma_i}{\gamma_i^*}) + 2(p+1)\gamma_{p+1}Y = Y(n+p+1) + \sum_{i=1}^{P} 2i\cdot\gamma_i^*\cdot\hat{X}_i .$$

Next we prove that the following 3 equations are equivalent (we use $\alpha_i^*\cdot\frac{\gamma_i}{\gamma_i^*} = \alpha_i$):

$$\alpha_i^* X_i = X_{p+1}\alpha_{p+1}^* + \sum_{t=i+1}^{p+1} 2(t-i)\gamma_i^* X_i$$

$$\alpha_i^*\hat{X}_i + \alpha_i Y = Y\alpha_{p+1} + \sum_{t=i+1}^{P} 2(t-i)\gamma_i^*\hat{X}_i + Y\sum_{t=i+1}^{p+1} 2(t-i)\gamma_i$$

$$\hat{X}_i\alpha_i^* = Y(p+1-i) + \sum_{t=i+1}^{P} 2(t-i)\gamma_i^*\hat{X}_i + Z$$

where $Z = Y(-\alpha_i + \alpha_{p+1} + \sum_{t=i+1}^{p+1} 2(t-i)\gamma_i + i - (p+1))$ .

$Z = 0$ follows from the definition of $\alpha_{p+1}$ and $\alpha_i$. Hence, the proof of the claim is complete. Hence, the proof of the theorem is complete. For later use we observe:

(5.9) $X_{p+1}\gamma_{p+1}^*$ is the least $Y$ such that $\psi^Y(A) = A$.

In the case $\gamma_{p+1} > 1$ this follows from (5.4) and (5.8). Q.E.D.

## 6. The possible periods

In this section we will find the possible periods of elements in $\mathfrak{M}$. First we introduce more notation.

Def. 6.1: a) Suppose $\mu = \gamma \times \gamma^*$ where $\gamma = (\gamma_1,\ldots,\gamma_{p+1})$ and $\gamma^* = (\gamma_1^*,\ldots,\gamma_{p+1}^*)$. We define

$$\alpha_i(\gamma) = n+i - \sum_{t=1}^{i} 2t\,\gamma_t - 2i\sum_{t=i+1}^{p+1}\gamma_t ,$$

$$\alpha_i^*(\mu) = \frac{\gamma_i^*}{\gamma_i}\cdot\alpha_i(\gamma) , \quad \gamma_i^*(\mu) = \gamma_i^* \text{ and } \gamma_i(\mu) = \gamma_i .$$

If $\gamma_i = 0$ for $i = 1,\ldots,p$, we let $X_{p+1}(\mu) = 1$ and $X_1(\mu) = \ldots = X_p(\mu) = 0$. Otherwise, we let $X_1(\mu),\ldots,X_{p+1}(\mu)$ be the least integral solution of the equations (1),...,(p) in the Thm. 5.1 with $\alpha_i^* = \alpha_i^*(\mu)$ and $\gamma_i^* = \gamma_i^*(\mu)$.

Moreover, we let

$$MP(\mu) = X_{p+1}(\mu)\alpha_{p+1}^*(\mu) + \sum_{i=1}^{p+1} 2i\,X_i(\mu)\gamma_i^*(\mu) .$$

b) For each $A \in \mathfrak{M}$, we define $\gamma(A) = (\gamma_1(A),\ldots,\gamma_{p+1}(A))$, $\gamma^*(A) = (\gamma_1^*(A),\ldots,\gamma_{p+1}^*(A))$ and $\mu(A) = \gamma(A)\times\gamma^*(A)$. Moreover, we let

$$\mathcal{P}_1 = \{\gamma(A): A \in \mathfrak{M}\} \text{ and } \mathcal{P}_2(\gamma) = \{\gamma^*(A): A \in \mathfrak{M} \text{ and } \gamma(A) = \gamma\} .$$

Theorem 6.2 follows from Theorem 5.1:

Theorem 6.2: The possible minimal periods of elements in $\mathfrak{M}$ are $\{MP(\mu): \mu \in \mathcal{P}\}$ where

$$\mathcal{P} = \bigcup_{\gamma \in \mathcal{P}_1} \gamma \times \mathcal{P}_2(\gamma) .$$

In the next theorem we construct $\mathcal{P}_1$ and $\mathcal{P}_2(\gamma)$ for each $\gamma \in \mathcal{P}_1$.

Theorem 6.3: a) $\gamma = (\gamma_1,\ldots,\gamma_{p+1}) \in \mathcal{P}_1$ if and only if there exists $m \geq 0$ such that

$$m + \sum_{i=1}^{p+1} i\cdot\gamma_i = k+p+1\,, \quad m + 2\sum_{i=1}^{p+1} i\cdot\gamma_i \leq n+p+1 \quad \text{and} \quad \gamma_{p+1} \neq 0\,.$$

We denote $m$ by $m(\gamma)$.

b) Let $\gamma = (\gamma_1,\ldots,\gamma_{p+1}) \in \mathcal{P}_1$. For $i = 1,\ldots,p$ we define

$$\Omega_i(\gamma) = \{\frac{\gamma_i}{r} : \frac{\gamma_i}{r} \text{ and } \frac{\alpha_i(\gamma)}{r} \text{ are integers}\}\,.$$

Moreover, we let

$$\Omega_{p+1}(\gamma) = \{\frac{\gamma_{p+1}}{r} : \frac{\gamma_{p+1}}{r}\,, \frac{\alpha_{p+1}(\gamma)}{r} \text{ and } \frac{m(\gamma)}{r} \text{ are integers}\}\,.$$

Then $\mathcal{P}_2(\gamma) = \prod_{i=1}^{p+1} \Omega_i(\gamma)$.

In the proof we need the following definition and lemma.

Def. 6.4: Suppose $\gamma \in \mathcal{P}_1$. Let $\mathcal{M}(\gamma) = \{A\in\mathcal{M} : (\gamma_1(A),\ldots,\gamma_{p+1}(A)) = \gamma\}$. For $i = 1,\ldots,p$ we define

$$\mathcal{N}_i(\gamma) = \{(d_1,\ldots,d_{\gamma_i}) : d_1 > 0,\ d_i \geq 0\ (i = 2,\ldots,\gamma_i) \text{ and } d_1+\ldots+d_{\gamma_i} = \alpha_i(\gamma)\}\,.$$

Moreover, we define

$$\mathcal{N}_{p+1}(\gamma) = \Big\{\Big[\binom{d_1}{s_1},\ldots,\binom{d_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\Big] : d_1+\ldots+d_{\gamma_{p+1}} = \alpha_{p+1}(\gamma) - m(\gamma)$$

$$s_1+\ldots+s_{\gamma_{p+1}} = m(\gamma)\,,\ d_i \geq 0 \text{ and } s_i \geq 0\Big\}\,.$$

Lemma 6.5: a) For $i = 1,\ldots,p$ we define $\rho_i : \{D_i(A) : A\in\mathcal{M}(\gamma)\} \to$ $\to \mathcal{N}_i(\gamma)$ by $\rho_i(t_1,\ldots,t_{\gamma_i}) = (t_1 - t_{\gamma_i} + \alpha_i(\gamma),\ t_2 - t_1,\ldots,t_{\gamma_i} - t_{\gamma_i-1})$. Then $\rho_i$ is surjective.

b) We define $\rho_{p+1}:\{D_{p+1}(A) : A \in \mathfrak{M}(\gamma)\} \to \mathfrak{N}_{p+1}(\gamma)$ by

$$\rho_{p+1}\left[\binom{t_1}{s_1},\ldots,\binom{t_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\right] = \left[\binom{d_1}{s_1},\ldots,\binom{d_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\right] \quad \text{where}$$

$$d_i = \begin{cases} t_1 & \text{if } i = 1 \\ t_i - t_{i-1} - s_{i-1} & \text{if } i \neq 1 . \end{cases}$$

Then $\rho_{p+1}$ is bijective.

Proof of Lemma 6.5: a) By Lemma 4.1 c) in [2]

$$\{D_i(A): A \in \mathfrak{M}(\gamma)\} = \{(t_1,\ldots,t_{\gamma_i}) : 0 < t_1 \leqq t_2 \leqq \ldots \leqq t_{\gamma_i} = \alpha_i(\gamma)\}$$

and the proof is obvious.

b) By Lemma 4.1 c) in [2]

$$\{D_{p+1}(A): A \in \mathfrak{M}(\gamma)\} = \Big\{\Big[\binom{t_1}{s_1},\ldots,\binom{t_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\Big] : 0 \leqq s_i,\ 0 \leqq t_i,$$

$t_i+s_i \leqq t_{i+1}$ $(i = 1,\ldots,\gamma_{p+1}-1)$, $t_{\gamma_{p+1}}+s_{\gamma_{p+1}} = \alpha_{p+1}(\gamma)$ and

$s_1+\ldots+s_{\gamma_{p+1}} = m(\gamma)\Big\}$. We observe that $\rho_{p+1}$ is well defined.

Let $D = [\binom{d_1}{s_1},\ldots,\binom{d_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}] \in \mathfrak{N}_{p+1}(\gamma)$. There exists one and only one $E$ such that $\rho_{p+1}(E) = D$. This $E$ can be constructed in the following way:

Put $E = [\binom{t_1}{s_1},\ldots]$ where $t_1 = d_1$, $t_2 = d_2 + t_1 + s_1$,

$t_3 = d_3 + t_2 + s_2$ etc. Q.E.D.

Proof of Thm. 6.3: a) follows from Lemma 4.1 c) in [2].

b) We observe $(i = 1,\ldots,p+1)$

(6.3) {the trivial period of $E$ : $E \in \mathfrak{N}_i(\gamma)$} $= \Omega_i(\gamma)$.

Moreover,

(6.4) $\gamma_i^*(A)$ is the trivial period of $\rho_i(D_i(A))$.

For $i = 1,\dots,p$ (6.4) follows directly from the definition. Next we let $i = p+1$ and $D_{p+1}(A) = [\binom{t_1}{s_1},\dots,\binom{t_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}]$. By definition $\gamma^*_{p+1}(A)$ is the trivial period of $[\binom{d_1'}{s_1},\dots]$ where

$$d_i' = \begin{cases} t_1 - t_{\gamma_{p+1}} + \alpha_{p+1}(\gamma) & \text{if } i = 1 \\ t_i - t_{i-1} & \text{if } i \neq 1 . \end{cases}$$

We denote $\rho_{p+1}(D_{p+1}(A)) = [\binom{d_1}{s_1},\dots]$. Since $s_{\gamma_{p+1}} + t_{\gamma_{p+1}} = \alpha_{p+1}(\gamma)$ (by Lemma 4.1 in [2]), we have $d_i = d_i' - s_{i-1}$ for $i = 1,\dots,p+1$ $(s_0 = s_{\gamma_{p+1}})$. Hence, $\gamma^*_{p+1}(A)$ is the trivial period of $\rho_{p+1}(D_{p+1}(A))$.

Lemma 6.5, (6.3) and (6.4) imply

$$\{\gamma_i^*(A) : A \in \mathcal{M}(\gamma)\} = \Omega_i(\gamma) \tag{6.5}$$

By Lemma 4.1 c) in [2]

$$\{D_1(A),\dots,D_{p+1}(A)) : A \in \mathcal{M}(\gamma)\} = \bigtimes_{i=1}^{p+1} \{D_i(A) : A \in \mathcal{M}(\gamma)\}. \tag{6.6}$$

(6.5) and (6.6) imply that b) is true. Q.E.D.

## 7. The number of cycles

In this section we will count the number of cycles in

$$\bar{\mathcal{M}} = \{A \in \{0,1\}^n : \exists\, i \text{ such that } \theta^i(A) \in \mathcal{M}\}$$

where $\mathcal{M}$ is defined in Section 4. First we do the following observation.

Observation 7.1: Suppose $\mathcal{C}$ is a cycle in $\bar{\mathcal{M}}$. If $A,B \in \mathcal{C} \cap \mathcal{M}$, then $\mu(A) = \mu(B)$.

Proof: There exists $i$ such that $\psi^i(A) = B$. By Obs. 3.10, Lemma 4.2 and 4.3 the observation follows. Q.E.D.

Next we let

(7.1) $G(\mu)$ = the number of cycles $\mathcal{C}$ in $\overline{\mathfrak{M}}$ such that $A \in \mathcal{C} \cap \overline{\mathfrak{M}} \Rightarrow \mu(A) = \mu$.

Theorem 7.2: For each $\mu \in \mathcal{P}$ we let $\gamma_i(\mu)$, $\alpha_i^*(\mu)$, $\gamma_i^*(\mu)$, $X_i(\mu)$, $MP(\mu)$ and $m(\mu)$ be as in Section 6. Moreover, we let $m^*(\mu) = m(\mu)\cdot\gamma_{p+1}^*(\mu)/\gamma_{p+1}(\mu)$.

a) The number of cycles in $\overline{\mathfrak{M}} = \Sigma\{G(\mu): \mu \in \mathcal{P}\}$.

b) The number of cycles in $\overline{\mathfrak{M}}$ of length $MP = \Sigma\{G(\mu): \mu \in \mathcal{P}$ and $MP(\mu) = MP\}$.

c) We let $\sigma(r,s,t)$ = the number of elements in

$\mathcal{R}(r,s,t) = \{(d_1,\ldots,d_s): d_i \geq 0,\ d_1 = r,\ d_1+\ldots+d_s = t$ and $(d_1,\ldots,d_s)$ has trivial period $s\}$.

Then $\sigma(r,s,t)$ can be calculated inductively by the following formula:

$$\sigma(r,s,t) = \binom{t+s-r-2}{s-2} - \Sigma\{\sigma(r,\tfrac{s}{s'},\tfrac{t}{s'}): \tfrac{s}{s'} \text{ and } \tfrac{t}{s'} \text{ are integers}\}.$$

$\binom{\ }{\ }$ is the binomial coefficient.

d) We let $\sigma(s,t)$ = the number of elements in

$\mathcal{R}(s,t) = \{(d_1,\ldots,d_s): d_i \geq 0,\ d_1+\ldots+d_s = t$ and $(d_1,\ldots,d_s)$ has trivial period $s\}$.

Then $\sigma(s,t)$ can be calculated inductively by the following formula:

$$\sigma(s,t) = \binom{t+s-1}{s-1} - \Sigma\{\sigma(\tfrac{s}{s'},\tfrac{t}{s'}): \tfrac{s}{s'} \text{ and } \tfrac{t}{s'} \text{ are integers}\}$$

e) $$G(\mu) = \left(\prod_{i=1}^{p+1} w_i(\mu)\right)\cdot\left(X_{p+1}(\mu)\gamma_{p+1}^*(\mu)\right)^{-1}$$

where (we write $\alpha_i^* = \alpha_i^*(\mu)$, $\gamma_i^* = \gamma_i^*(\mu)$ and $m^* = m^*(\mu)$)

$$w_i(\mu) = \sum_{t=1}^{\alpha_i^*} t\cdot\sigma(t,\gamma_i^*,\alpha_i^*) \qquad \text{for } i = 1,\ldots,p$$

and

$$w_{p+1}(\mu) = \sigma(\gamma_{p+1}^*,\alpha_{p+1}^*-m^*)\cdot\binom{m^*+\gamma_{p+1}^*-1}{\gamma_{p+1}^*-1}$$
$$+\binom{\alpha_{p+1}^*-m^*+\gamma_{p+1}^*-1}{\gamma_{p+1}^*-1}\cdot\sigma(\gamma_{p+1}^*,m^*) - \sigma(\gamma_{p+1}^*,\alpha_{p+1}^*-m^*)\cdot\sigma(\gamma_{p+1}^*,m^*).$$

Proof: In the proof we let # denote "the number of elements in".

a) and b) follows from Thm. 6.2 and Obs. 7.1.

c) $\{(d_1,\ldots,d_s)$: $d_i \geq 0$, $d_1 = r$ and $d_1+\ldots+d_s = t\}^{\#}$
$= \{(d_2,\ldots,d_s)$: $d_i \geq 0$ and $d_2+\ldots+d_s = t-r\}^{\#}$
= the number of ways to divide $(t-r)$ 1's into $(s-1)$ groups
= the number of ways to put $s-2$ 0's into $(t+s-r-2)$ positions
$= \binom{t+s-r-2}{s-2}$.

We subtract those $(d_1,\ldots,d_s)$ with trivial period less than $s$. For each $s'$ such that $\frac{s}{s'}$ and $\frac{t}{s'}$ are integers, $(d_1,\ldots,d_s) \to (d_1,\ldots,d_{s/s'})$ is a bijective correspondence between

$\{(d_1,\ldots,d_s)$: $0 \leq d_i$, $d_1 = r$, $d_1+\ldots+d_s = t$ and
$(d_1,\ldots,d_s)$ has trivial period $s/s'\}$

and $\mathcal{R}(r,s/s',t/s')$.

By using these correspondences c) follows.

d) The proof of d) is analogous with the proof of c).

e) We let $\eta_i(\gamma)$ and $\rho_i$ be as in Section 6. First we introduce some notation and observations. If $\mu = \gamma\times\gamma^*$ $(\gamma_1,\ldots,\gamma_{p+1})\times(\gamma_1^*,\ldots,\gamma_{p+1}^*)$ we let for $i = 1,\ldots,p$

$$\eta_i(\mu) = \{(d_1,\ldots,d_{\gamma_i}) \in \eta_i(\gamma) : (d_1,\ldots,d_{\gamma_i}) \text{ has trivial period } \gamma_i^*\}.$$

Moreover,

$$\eta_{p+1}(\mu) = \left\{\left[\binom{d_1}{s_1},\ldots,\binom{d_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\right] \in \eta_{p+1}(\gamma) \text{ with trivial period } \gamma_{p+1}^*\right\}.$$

By Lemma 6.5 we prove easily

$$(7.2)\quad \begin{cases} \rho_i\colon \{D_i(A)\colon \mu(A) = \mu\} \to \eta_i(\mu) \text{ is surjective} \\ \quad \text{for } i = 1,\ldots,p \text{ and bijective for } i = p+1 . \end{cases}$$

Suppose $i \in \{1,\ldots,p\}$. If $(d_1,\ldots,d_{\gamma_i}) \in \eta_i(\mu)$, then

$$d_1+\ldots+d_{\gamma_i^*} = d_{\gamma_i^*+1}+\ldots+d_{2\gamma_i^*} = \ldots = d_{(r-1)\gamma_i^*+1}+\ldots+d_{r\gamma_i^*} = \frac{\alpha_i(\gamma)}{r} = \alpha_i^*(\mu) \quad \text{since} \quad r = \frac{\gamma_i}{\gamma_i^*}.$$

Specially we have

$$(7.3)\qquad d_1 \leq \alpha_i^*(\mu) \quad \text{for} \quad (d_1,\ldots,d_{\gamma_i}) \in \eta_i(\mu).$$

Next we do the following observation ($i = 1,\ldots,p$):

(7.4) To each $(d_1,\ldots,d_{\gamma_i}) \in \eta_i(\mu)$ there exists exactly $d_1$ elements $D \in \{D_i(A)\colon \mu(A) = \mu\}$ such that $\rho_i(D) = (d_1,\ldots,d_{\gamma_i})$.

These elements are

$$(s,\ s+d_2,\ s+d_2+d_3,\ldots,s+\sum_{j=2}^{\gamma_i} d_j) \quad \text{where} \quad s = 1,\ldots,d_1 .$$

Now we start the proof. (5.9) in the proof of Thm. 5.1 implies that for each $A \in \mathfrak{M}$ such that $\mu(A) = \mu$ we have:

There are $X_{p+1}(\mu)\gamma_{p+1}^*(\mu)$ elements in $\mathfrak{M}$ on the same cycle as $A$.

Hence, we must prove $\{A \in \mathfrak{M} : \mu(A) = \mu\}^{\#} = \prod_{i=1}^{p+1} w_i(\mu)$ .

By Lemma 4.1 c) in [2] we have

$$\bigtimes_{i=1}^{p+1} \{D_i(A) : \mu(A) = \mu\} = \{(D_1(A),\ldots,D_{p+1}(A)) : \mu(A) = \mu\}$$

and

$$\{(D_1(A),\ldots,D_{p+1}(A)) : \mu(A) = \mu\}^{\#} = \{A \in \mathfrak{M} : \mu(A) = \mu\}^{\#} .$$

Hence, the proof is complete if we can prove

$$(7.5) \qquad \{D_i(A) : \mu(A) = \mu\}^{\#} = w_i(A) \qquad \text{for } i = ,\ldots, p+1 .$$

We suppose first $1 \leqq i \leqq p$ . By (7.2), (7.3) and (7.4) we get

$$\{D_i(A) : \mu(A) = \mu\}^{\#} = \prod_{r=1}^{\alpha_i^*} (t \cdot \{(d_1,\ldots,d_{\gamma_i}) \in \mathfrak{N}_i(\mu) : d_1 = t\}^{\#}) .$$

Hence, we must prove

$$\{(d_1,\ldots,d_{\gamma_i}) \in \mathfrak{N}_i(\mu) : d_1 = t\}^{\#} = \sigma(t,\gamma_i^*,\alpha_i^*) .$$

This follows by c) since $\{(d_1,\ldots,d_{\gamma_i}) \in \mathfrak{N}_i(\mu) : d_1 = t\}$ is in bijective correspondence with $\mathfrak{R}(t,\gamma_i^*,\alpha_i^*)$ by the map $(d_1,\ldots,d_{\gamma_i}) \to (d_1,\ldots,d_{\gamma_i^*})$ .

Hence, (7.5) is proved in the case $1 \leqq i \leqq p$ .

Next we prove (7.5) in the case $i = p+1$ . By (7.2)

$$(7.6) \qquad \{D_{p+1}(A) : \mu(A) = \mu\}^{\#} = \mathfrak{N}_{p+1}(\mu)^{\#}$$

We let

$$Q(s,t) = \{(d_1,\ldots,d_s) : d_i \geqq 0 \text{ and } d_1+\ldots+d_s = t\} .$$

We get

$$(7.7) \qquad Q(s,t)^{\#} = \binom{s+t-1}{s-1} .$$

We define

$$\Phi\left(\left[\binom{d_1}{s_1},\ldots,\binom{d_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\right]\right) = (d_1,\ldots,d_{\gamma^*_{p+1}}) \times (s_1,\ldots,s_{\gamma^*_{p+1}})$$

for elements in $\mathcal{N}_{p+1}(\mu)$.

$\Phi$ is injective and $\Phi(\mathcal{N}_{p+1}(\mu)) =$

$$\mathcal{R}(\gamma^*_{p+1},\alpha^*_{p+1}-m^*) \times Q(\gamma^*_{p+1},m^*) \cup Q(\gamma^*_{p+1},\alpha^*_{p+1}-m^*) \times \mathcal{R}(\gamma^*_{p+1},m^*)$$

Hence, by d) and (7.7) we get

$$(7.8) \qquad \mathcal{N}_{p+1}(\mu)^{\#} = w_{p+1}(\mu) .$$

In the proof of (7.8) we use the formula

$$(A \cup B)^{\#} = A^{\#} + B^{\#} - (A \cap B)^{\#} .$$

(7.6) and (7.8) imply $\{D_{p+1}(A) : \mu(A) = \mu\}^{\#} = w_{p+1}(\mu)$.

Q.E.D.

## 8. The reduction

We will reduce the cycle structure problem to the set studied in the Sections 4 - 7. First we need two lemmas. $C < D$ means $C$ contained in $D$ and $C \neq D$. If $D = a_r \ldots a_s$, we define $(t \in D \Leftrightarrow r \leqq t \leqq s)$ and $f_D(t) = f(a_r \ldots a_t)$.

Lemma 8.1: Suppose $A = O_{i_1} B_1 C_1 O_{i_2} B_2 C_2 \ldots O_{i_f} B_f$ where $B_i$ is a block on level 1. Moreover, we suppose $f(C_i) = -\text{type}(B_i)$ and $0 > f_{C_i}(t) \geqq -\text{type}(B_i)$ for $t \in C_i$.

Then we have

$$n + \text{type}(B_f) = \left(\sum_{i=1}^{p+1} 2i\,\gamma_i\right) + m_A + (i_1+\ldots+i_f) ,$$

and

$$\alpha_{\text{type}(B_f)}(A) = m_A \Leftrightarrow i_1+\ldots+i_f = 0 .$$

Proof: We let $C_f = 0_{type(B_f)}$ and consider

$A^* = AC_f = 0_{i_1}B_1C_1 \ldots 0_{i_f}B_fC_f$ .

As in the proof of Lemma 4.13 in [2] we get

the length of $B_i = m(B_i) + \Sigma\{2\cdot type(B^*): B^* < B_i\}$ ,

the length of $C_i = type(B_i) + \Sigma\{2\cdot type(B^*): B^* < C_i\}$ .

If $type(B_i) = p+1$ , we therefore have

the length of $B_iC_i = [m(B_i)-(p+1)] + \Sigma\{2\cdot type(B^*): B^* < B_iC_i\}$ .

Otherwise,

the length of $B_iC_i = \Sigma\{2\cdot type(B^*): B^* < B_iC_i\}$ .

Hence,

the length of $A^* = \Sigma\{m(B_i)-(p+1): type(B_i) = p+1\}$

$+ \Sigma\{2\cdot type(B^*): B^* \text{ a block}\} + (i_1+\ldots+i_f)$

$= m_A + (\sum_{i=1}^{p+1} 2i\,\gamma_i) + (i_1+\ldots+i_f)$ .

The equivalence follows by the definition of $\alpha_{type(B_f)}(A)$ .

Q.E.D.

We write

(8.1) $$\theta_{k,p} = \theta_{E_k+\ldots+E_{k+p}} .$$

Lemma 8.2: We suppose the block structure of $A \in \{0,1\}^n$ is determined with respect to $p$ . Moreover, we suppose $w(A) = k+p+1$ .

Then we have

$([\gamma_{p+1}(A) \neq 0$ and $\alpha_{p+1}(A) = m_A]$ or $[z = \sup_i\{i : \gamma_i(A) \neq 0\} < p+1$ and $\alpha_z(A) = 0]) \Leftrightarrow \theta^j_{k,p}(A) = \theta^j_{k,p'}(A)$ for $p' > p$ and every $j$ .

Proof: We suppose first $\gamma_{p+1}(A) \neq 0$. By Lemma 4.4 in [2] there exists $q$ such that $\bar{A} = \theta^q_{k,p}(A)$ satisfies

$\gamma_i(A) = \gamma_i(\bar{A})$, $\alpha_i(A) = \alpha_i(\bar{A})$, $m_A = m_{\bar{A}}$, $\bar{A}$ ends with a $(p+1)$-block, $\bar{A}$ starts with 0 or a $(p+1)$-block and $w(\bar{A}) = k+p+1$.

Moreover, $\bar{A}$ has the form

$\bar{A} = 0^{i_1}B_1C_1 0^{i_2}B_2C_2 \ldots 0^{i_f}B_f$ as in Lemma 8.1.

(If $f = 1$, then $\bar{A} = 0^{i_1}B_1$.)

We suppose $\theta^j_{k,p}(A) = \theta^j_{k,p'}(A)$ for $p' > p$. If $i_1 \neq 0$, then $w(\theta_{k,p+1}(A)) = k+p+2 \neq w(\theta_{k,p}(A))$. Hence, $i_1 = 0$. By Lemma 5.7 in [2] we have

$w(\theta^s_{k,p}(\bar{A})) = k+p+1$ where $s$ = length of $B_1C_1$.

In the same way we prove $i_1 = \ldots = i_f = 0$. By Lemma 8.1 $\alpha_{p+1}(\bar{A}) = m_{\bar{A}}$. Hence, $\alpha_{p+1}(A) = m_A$.

Next we suppose $\alpha_{p+1}(A) = m_A$. Hence, $\alpha_{p+1}(\bar{A}) = m_{\bar{A}}$. By Lemma 8.1 we have $i_1 + \ldots + i_f = 0$. Hence, $\text{type}(B_1) = p+1$. Moreover, let $j = \inf\{i > 1 : \text{type}(B_i) = p+1\}$. Put $C_1 "=" C_1B_2C_2 \ldots B_{j-1}C_{j-1}$ and $B_2 "=" B_j$. By continuing in this way we can suppose $\text{type}(B_1) = \ldots = \text{type}(B_f) = p+1$. Hence, by Lemma 5.6 c) we get $\theta^j_{k,p}(\bar{A}) = \theta^j_{k,p'}(\bar{A})$ for $p' > p$.

Finally we treat the case $z = \sup_i \gamma_i(A) < p+1$. By Lemma 5.6 a) we have $\theta^j_{k,p}(A) = \theta^j_{k_1,p_1}(A)$ where $k_1 = p+1-z$ and $p_1 = z-1$. By Lemma 4.4 in [2] there exists $q$ such that $\bar{A} = \theta^q_{k,p}(A)$ satisfies:

$\gamma_i(A) = \gamma_i(\bar{A})$, $\alpha_i(A) = \alpha_i(\bar{A})$, $m_A = m_{\bar{A}} = 0$, $\bar{A}$ ends with a $z$-block, $\bar{A}$ starts with 0 or a $z$-block and $w(\bar{A}) = k+p+1$. Moreover, $\bar{A}$ has the form

$\bar{A} = 0^{i_1}B_1C_1 0^{i_2}B_2C_2 \ldots 0^{i_f}B_f$ as in Lemma 8.1.

We suppose $\theta^j_{k,p}(A) = \theta^j_{k,p'}(A)$ for $p' > p$. As in the case $\gamma_{p+1}(A) \neq 0$ we prove $i_1 = \ldots = i_f = 0$. By Lemma 8.1 $\alpha_z(A) = m_A = 0$.

Next we suppose $\alpha_z(A) = 0$. Hence, $\alpha_z(\bar{A}) = m_{\bar{A}} = 0$. By Lemma 8.1 we have $i_1 + \ldots + i_f = 0$. As before we can suppose $\text{type}(B_1) = \ldots = \text{type}(B_f) = z$. Hence, by Lemma 5.6 c) we get $\theta^j_{k,p}(\bar{A}) = \theta^j_{k,p'}(\bar{A})$ for $p' > p$.

Q.E.D.

Now we start the reduction process. We need very precise notation:

If we determine the block structure of $A$ with respect to $p$, we write $\gamma^p_i(A) = \gamma_i(A)$, $\alpha^p_i(A) = \alpha_i(A)$ and $m^p_A = m_A$.

For $\mathcal{F} \subset \{0,1\}^n$ we define $\mathcal{F}^{[k,p]} = \{\theta^i_{k,p}(A) : A \in \mathcal{F}$ and $i$ is an integer$\}$.

Reduction 1: We define

$$\mathfrak{M}_{k,p} = \{A : w(A) = \sup_i w(\theta^i_{k,p}(A)) \in \{k, \ldots, k+p+1\}\}.$$

If $A = a_1 \ldots a_n \notin \mathfrak{M}^{[k,p]}_{k,p}$, then we have $\theta_{k,p}(A) = a_2 \ldots a_n a_1$ and $\theta_{k,p}(A) \notin \mathfrak{M}^{[k,p]}_{k,p}$.

Proof: For $A = a_1 \ldots a_n \notin \mathfrak{M}^{[k,p]}_{k,p}$ we have $w(a_2 \ldots a_n) \notin \{k, \ldots, k+p\}$. Hence, $(E_k + \ldots + E_{k+p})(a_2 \ldots a_n) = 0$.

Q.E.D.

Reduction 2: We define

$$\mathfrak{M}_{k,p}(i) = \{A \in \mathfrak{M}_{k,p} : w(A) = i\}.$$

a) $\mathfrak{M}^{[k,p]}_{k,p} = \bigcup_{s=0}^{p} \mathfrak{M}_{k,p}(k+s+1)^{[k,p]}$ is a disjoint union.

b) We define

$$\mathfrak{M}^{*}_{k,p}(k+p+1) = \{A \in \mathfrak{M}_{k,p}(k+p+1) : (\gamma^{p}_{p+1}(A) \neq 0 \quad \text{and}$$

$$\alpha^{p}_{p+1}(A) = m^{p}_{A}) \quad \text{or} \quad (z = \sup\{i : \gamma^{p}_{i}(A) \neq 0\} < p+1 \quad \text{and}$$

$$\alpha^{p}_{z}(A) = 0)\} .$$

For $s < p$ we have

$$\mathfrak{M}_{k,p}(k+s+1)^{[k,p]} = \mathfrak{M}^{*}_{k,s}(k+s+1)^{[k,s]} \quad \text{and}$$

$$\theta_{k,p} = \theta_{k,s} \quad \text{on this set.}$$

Proof: a) is obvuous.

b) By Lemma 5.6 c) in [2] we have $\theta^{i}_{k,p}(A) = \theta^{i}_{k,s}(A)$ for all $i$ and $A \in \mathfrak{M}_{k,p}(k+s+1)$. Moreover, by Lemma 8.2 we have

$$A \in \mathfrak{M}_{k,p}(k+s+1) \iff A \in \mathfrak{M}^{*}_{k,s}(k+s+1) .$$

Q.E.D.

By Reduction 2 it is sufficient to determine the cycle-structure of the sets

$$\mathfrak{M}_{k,p}(k+p+1)^{[k,p]} \quad \text{and} \quad \mathfrak{M}^{*}_{k,p}(k+p+1)^{[k,p]}$$

with respect to $\theta_{k,p}$.

Reduction 3: We define

$$\mathfrak{M}_{k,p}(k+p+1,j) = \{A \in \mathfrak{M}_{k,p}(k+p+1) : \sup\{i:\gamma^{p}_{i}(A) \neq 0\} = j\},$$

$$\mathfrak{M}^{*}_{k,p}(k+p+1,j) = \{A \in \mathfrak{M}^{*}_{k,p}(k+p+1) : \sup\{i:\gamma^{p}_{i}(A) \neq 0\} = j\}.$$

a) $\mathfrak{M}_{k,p}(k+p+1)^{[k,p]} = \bigcup_{j=1}^{p+1} \mathfrak{M}_{k,p}(k+p+1,j)^{[k,p]}$ is a disjoint union.

b) Suppose $j < p+1$. Put $k' = k+p+1-j$ and $p' = j-1$.

Then

$$\mathfrak{M}_{k,p}(k+p+1,j)^{[k,p]} = \{A \in \mathfrak{M}_{k',p'}(k'+p'+1,p'+1) : m_A^{p'} = 0\}^{[k',p']}$$

and $\theta^i_{k,p}(A) = \theta^i_{k',p'}(A)$ for $A \in \mathfrak{M}_{k,p}(k+p+1,j)$.

c) $\mathfrak{M}^*_{k,p}(k+p+1)^{[k,p]} = \bigcup_{j=1}^{p+1} \mathfrak{M}^*_{k,p}(k+p+1,j)^{[k,p]}$ is a disjoint union.

d) Suppose $j < p+1$. Put $k' = k+p+1-j$ and $p' = j-1$.

Then

$$\mathfrak{M}^*_{k,p}(k+p+1,j)^{[k,p]} = \{A \in \mathfrak{M}_{k',p'}(k'+p'+1) : \alpha^{p'}_{p'+1}(A) = 0\}^{[k',p']}$$

and $\theta^i_{k,p}(A) = \theta^i_{k',p'}(A)$ for $A \in \mathfrak{M}^*_{k,p}(k+p+1,j)$.

e) $\mathfrak{M}^*_{k,p}(k+p+1,p+1)^{[k,p]} = \{A \in \mathfrak{M}_{k,p}(k+p+1,p+1) : \alpha^{p}_{p+1}(A) = m_A\}^{[k,p]}$.

Proof: By Lemma 4.12 in [2] we have for $A \in \mathfrak{M}_{k,p}$:

If $w(\theta^i_{k,p}(A)) = k+p+1$, then $\gamma_i(A) = \gamma_i(\bar{A})$, $\alpha_i(A) = \alpha_i(\bar{A})$ and $m_A = m_{\bar{A}}$ where $\bar{A} = \theta^i_{k,p}(A)$.

a) and c) follows from this observation. e) follows by the definition of $\mathfrak{M}^*_{k,p}(k+p+1)$.

b) By the definitions of blocks

$$A \in \mathfrak{M}_{k,p}(k+p+1,j) \Leftrightarrow A \in \mathfrak{M}_{k',p'}(k'+p'+1,p'+1) \text{ and } m_A^{p'} = 0.$$

Moreover, by Lemma 5.6 a) in [2] we have

(8.2) $\theta^i_{k,p}(A) = \theta^i_{k',p'}(A)$ for all $i$ and $A \in \mathfrak{M}_{k,p}(k+p+1,j)$.

d) By the definition of $\mathfrak{M}^*_{k,p}(k+p+1,j)$

$$A \in \mathfrak{M}^*_{k,p}(k+p+1,j) \Leftrightarrow A \in \mathfrak{M}_{k',p'}(k'+p'+1,p'+1) \text{ and } \alpha^{p'}_{p'+1}(A) = 0$$

and d) follows.

Q.E.D.

Put $\mathcal{N} = \mathcal{M}_{k,p}(k+p+1,p+1)$. By the Reduction 3 there is sufficient to determine the cycle structure with respect to $\theta_{k,p}$ of the following 4 sets

$$\mathcal{N}^{[k,p]},$$

$$\mathcal{G}_1 = \{A \in \mathcal{N} : m_A^p = 0\}^{[k,p]},$$

$$\mathcal{G}_2 = \{A \in \mathcal{N} : \alpha_{p+1}^p(A) = 0\}^{[k,p]},$$

$$\mathcal{G}_3 = \{A \in \mathcal{N} : \alpha_{p+1}^p(A) = m_A\}^{[k,p]}.$$

By Lemma 4.4 in [2] $\mathcal{N}^{[k,p]} = \mathcal{M}^{[k,p]}$ where $\mathcal{M}$ is as in Section 4. Hence, the cycle structure of $\mathcal{N}^{[k,p]}$ is completely determined in the Sections 4 - 7. The other 3 sets are subsets of $\mathcal{N}^{[k,p]}$ and we find the cycle structure of these sets by modifying the Theorems 6.2, 6.3 and 7.2. More precisely, let $\mathcal{P}_1$ be as in Thm. 6.3 and define.

$$\mathcal{P}_1^1 = \{(\gamma_1,\ldots,\gamma_{p+1}) \in \mathcal{P}_1 : \sum_{i=1}^{p+1} i\cdot\gamma_i = k+p+1 \text{ and } 2\sum_{i=1}^{p+1} i\cdot\gamma_i \leq n+p+1\}$$

$$\mathcal{P}_1^2 = \{(\gamma_1,\ldots,\gamma_{p+1}) \in \mathcal{P}_1 : \sum_{i=1}^{p+1} i\cdot\gamma_i = k+p+1 \text{ and } \sum_{i=1}^{p+1} 2\cdot i\cdot\gamma_i = n+p+1\}$$

$$\mathcal{P}_1^3 = \{\gamma = (\gamma_1,\ldots,\gamma_{p+1}) \in \mathcal{P}_1 : m(\gamma) + 2\sum_{i=1}^{p+1} i\,\gamma_i = n+p+1 \text{ and } m(\gamma) + \sum_{i=1}^{p+1} i\,\gamma_i = k+p+1\}$$

If we will determine the cycle structure of $\mathcal{G}_i$, the only change in the Theorems 6.2, 6.3 and 6.4 is that we replace $\mathcal{P}_1$ in Thm. 6.3 a) by $\mathcal{P}_1^i$ $(i = 1,2,3)$.

Next we do the following observations.

Observation 8.3: Thm. 5.1 is true for $A \in \{0,1\}^n$ such that $w(A) = k+p+1$ and $\gamma_{p+1}^p(A) \neq 0$.

Proof: By Lemma 4.4 and 4.12 in [2] there exists $j$ such that $A^* = \theta^j_{k,p}(A) \in \mathfrak{M}$ and integers $r_q, \chi_q$ $(q = 1,\ldots,p+1)$ such that:

$$\begin{cases} \text{If } q \in \{1,\ldots,p\} \text{ and } D_q(A) = (t_1,\ldots,t_{\gamma_q}), \text{ then} \\ D_q(A^*) = (t_{r_{q+1}}-\chi_q,\ldots,t_{\gamma_q}-\chi_q,t_1-\chi_q+\alpha_q(A),\ldots,t_{r_q}-\chi_q+\alpha_q(A)). \\ \text{Moreover, the analogous statement is true for } q = p+1. \end{cases}$$

It is very easy to see that the trivial periods of the difference vectors of $D_q(A)$ and $D_q(A^*)$ are equal. Hence, $\gamma^*_q(A) = \gamma^*_q(A^*)$ and $\alpha^*_q(A) = \alpha^*_q(A^*)$ for $q = 1,\ldots,p+1$.
The observation follows easily.

Q.E.D.

Observation 8.4: Suppose $w(A) \in \{k,\ldots,k+p+1\}$. Then

$$\sup_{1 \leqq i \leqq 2n} w(\theta^i_{k,p}(A)) = \sup_i w(\theta^i_{k,p}(A)).$$

Proof: We choose $j$ such that $A^* = \theta^j_{k,p}(A)$ satisfies $w(A^*) = \sup w(\theta^i_{k,p}(A))$. As in Step 3 and 4 in the forthcoming procedure where we determine the minimal periods, we can suppose $w(A^*) = k+p+1$ and $\gamma^p_{p+1}(A) \neq 0$. By Lemma 4.4 in [2] there exists $i$ such that $A^{**} = \theta^i_{k,p}(A^*) \in \mathfrak{M}$ where $\mathfrak{M}$ is as in Section 4.

By Lemma 4.2 and 4.3 we have

$$w(A^{**}) = w(\psi(A^{**})) = \ldots = w(\psi^j(A^{**})) = \ldots = k+p+1$$

and $\psi^j(A^{**}) = \theta^q_{k,p}(\psi^{j-1}(A^{**}))$ for some $q \leqq 2n$.

Hence, the observation follows.

Q.E.D.

Finally we will mention how to determine the minimal period for $A \in \{0,1\}^n$ with respect to $\theta_{k,p}$ in the following 4 steps:

1. If $w(A) \notin \{k,\ldots,k+p+1\}$, then $\theta_{k,p}(A) = \xi(A)$ where $\xi(a_1\ldots a_n) = (a_2\ldots a_n a_1)$ and the problem is trivial.

We therefore suppose $w(A) \in \{k,\ldots,k+p+1\}$.

2. We calculate $w(A), w(\theta_{k,p}(A)), \ldots, w(\theta^{2n}_{k,p}(A))$ and choose $j$ such that $A^* = \theta^j_{k,p}(A)$ satisfies

$$w(A^*) = \sup_{1\leq i\leq 2n} w(\theta^i_{k,p}(A)) = \sup_i w(\theta^i_{k,p}(A)) .$$

(The last equality follows from Obs. 8.4.)

3. Put $p' = w(A^*)-k-1$. Then we can use $\theta_{k,p'}$ instead of $\theta_{k,p}$ (Lemma 5.6 b) in [2]). We have $w(A^*) = k+p'+1$.

4. Next we determine the block structure of $A^*$ with respect to $p'$, We put $j = \sup\{i : \gamma^{p'}_i(A) \neq 0\}$, and $k" = p'-j$ and $p" = j-1$. Then we can use $\theta_{k",p"}$ instead of $\theta_{k,p}$ (Lemma 5.6 a) in [2]). Moreover, we have $w(A^*) = k"+p"+1$ and $\gamma^{p"}_{p"+1}(A^*) \neq 0$. Hence, we can use Thm. 5.1 (Obs. 8.3).

Index of notation:



References:


1. J. Søreng, The periods of the sequences generated by some shift registers, J. Combinatorial Theory, Ser. A.21(1976),165-187.

2. J. Søreng, Symmetric Shift Registers.

(This is a revised version of "The difference equation $x_{n+1} = x_1 + S(x_2,\ldots,x_n)\ldots$", Preprint No.19, 1977 University of Oslo.)

Appendix

In this appendix we will formulate the results in [2] which is not contained in "The difference equation ... ". First we mention that the definition of $d(B)$ is changed: If we denote $d(B)$ in "The difference equation ... " by $\hat{d}(B)$, then $d(B) = \hat{d}(B)-1$ where $d(B)$ is as in the revised version. Now we will formulate Lemma 4.1. c), 4.4 , 4.11 , 4.12 , 4.13 , 5.6 and 5.7 in [2]. The lemmas are reformulated slightly by using the notation of this paper. We refer to the index of notation.

Lemma 4.1 c): Suppose $\gamma = (\gamma_1,\ldots,\gamma_{p+1}) \in \mathcal{P}_1$ ( $\mathcal{P}_1$ is as in Thm. 6.3 a)). Then

$$\{(D_1(A),\ldots,D_{p+1}(A)) : A \in \mathcal{M}(\gamma)\} = \overset{p+1}{\underset{i=1}{X}} \mathcal{F}_i \quad \text{where}$$

$$\mathcal{F}_i = \{(t_1,\ldots,t_{\gamma_i}) : 0 < t_1 \leqq t_2 \leqq \ldots \leqq t_{\gamma_i} \leqq \alpha_i(\gamma)\} \qquad \text{for } i = 1,\ldots,p,$$

and

$$\mathcal{F}_{p+1} = \left\{\left[\binom{t_1}{s_1},\ldots,\binom{t_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\right] : t_1 \geqq 0,\ s_1 \geqq 0,\ s_1+\ldots+s_{\gamma_{p+1}} = m(\gamma),\right.$$

$$\left. t_i + s_i \leqq t_{i+1} \quad (i = 1,\ldots,\gamma_{p+1}-1) \text{ and } t_{\gamma_{p+1}} + s_{\gamma_{p+1}} = \alpha_{p+1}(\gamma)\right\}.$$

Moreover, $A$ is uniquely determined by $D_1(A),\ldots,D_{p+1}(A)$. Finally, we have

$$\mathcal{M} = \bigcup_{\gamma \in \mathcal{P}_1} \mathcal{M}(\gamma) .$$

Lemma 4.4: Suppose $w(A) = k+p+1$ and $A \in \{0,1\}^n$. Then there exists $j$ such that $A^* = \theta^j_{k,p}(A) \in \mathcal{M}$ and $\gamma_j(A) = \gamma_j(A^*)$ $(i = 1,\ldots,p+1)$ and $m_A = m_{A^*}$.

Lemma 4.11 is almost equal to Lemma 4.2 in this paper.

Lemma 4.12: Suppose $w(A) = w(\theta^i_{k,p}(A)) = k+p+1$. Put $A^* = \theta^i_{k,p}(A)$. Then there exists $r_q, \chi_q$ $(q = 1,\dots,p+1)$ such that:

If $1 \leqq q \leqq p$ and $D_q(A) = (t_1,\dots,t_{\gamma_q})$, then

$$D_i(A^*) = (t_{r_q+1}-\chi_q,\dots,t_{\gamma_q}-\chi_q, t_1+\alpha_q(A)-\chi_q, \dots, t_{r_q}+\alpha_q(A)-\chi_q) .$$

Moreover, if $D_{p+1}(A) = \left[\binom{t_1}{s_1},\dots,\binom{t_{\gamma_{p+1}}}{s_{\gamma_{p+1}}}\right]$, then

$$D_{p+1}(A) = \left[\binom{t_{r_q+1}-\chi_q}{s_{r_q+1}},\dots,\binom{t_{\gamma_q}-\chi_q}{s_{\gamma_q}},\binom{t_1+\alpha_q(A)-\chi_q}{s_1},\dots,\binom{t_{r_q}+\alpha_q(A)-\chi_q}{s_{r_q}}\right]$$

where $q = p+1$.

Lemma 4.13 is almost equal to Lemma 4.3 in this paper.

Lemma 5.6: a) We suppose $A \in \{0,1\}^n$ and $w(A) = k+p+1$. We determine the block structure of $A$ with respect to $p$. If $j = \sup\{\text{type}(B) : B \text{ block in } A\}$, then

$$w(\theta^i_S(A)) \geqq k+p+1-j \quad \text{and} \quad \theta^i_S(A) = \theta^i_{S'}(A) \quad \text{for every } i ,$$

where $S = E_k+\dots+E_{k+p}$, $S' = E_{k'}+\dots+E_{k'+p'}$, $p' = j-1$ and $k' = k+p+1-j$.

b) We suppose $A \in \{0,1\}^n$. $S = E_k+\dots+E_{k+p}$ and $w(A) = \sup_i w(\theta^i_S(A)) = k+p'+1$. Then $\theta^i_S(A) = \theta^i_{S'}(A)$ for every $i$, where $S' = E_k+\dots+E_{k+p'}$.

c) We suppose $A = a_1\dots a_n \in \{0,1\}^n$ and $w(A) = k+p+1$. Suppose $1 \leqq z \leqq p+1$. Suppose $A = B$ is a $z$-block or

$$\left\{\begin{array}{l} A = B_1T_1B_2T_2\dots B_f \text{ where } \text{type}(B_i) = z \text{ and } T_i = a_r\dots a_s \\ \text{satisfies} \\ 0 > f(a_r\dots a_j) \geqq -z = f(T_i) \quad \text{for } j = r,\dots,s \ (i = 1,\dots,f-1) . \end{array}\right.$$

Then for $p' > p$ we have $\theta^i_{S'}(A) = \theta^i_S(A)$ for every $i$, where $S' = E_k+\dots+E_{k+p'}$ and $S = E_k+\dots+E_{k+p}$.

Lemma 5.7: Suppose $A \in \{0,1\}^n$ and $w(A) = k+p+1$ and $S = E_k + \ldots + E_{k+p}$. Suppose $A = BTD$ where $B$ is a block and $T = a_r \ldots a_s$ satisfies

$$0 > f(a_r \ldots a_j) \geqq -\text{type}(B) = f(T) \quad \text{for} \quad j = r,\ldots,s .$$

Then $w(\theta_S^z(A)) = k+p+1$ where $z$ = the length of $BT$.